UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/673,847	09/30/2003	Xiaomang Zhang	0717-0518P	3716

2292 7590 07/02/2007
BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2132	

NOTIFICATION DATE	DELIVERY MODE
07/02/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

Office Action Summary	Application No.	Applicant(s)	
	10/673,847	ZHANG, XIAOMANG	
	Examiner	Art Unit	
	Thomas M. Ho	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 September 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/7/06, 9/30/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-31 are pending.

Claim Rejections - 35 USC § 112

2. Claims 3, 6, 8, 10, 11, 12, 16, 17, 21-26 rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential elements, such omission amounting to a gap between the elements. See MPEP § 2172.01. The omitted elements are:

Claim 16 recites a start signal, an external device, and a communication request ID but fails to disclose the structural cooperative relationships between the elements. For example, Claim 16 recites a start signal generation section but fails to disclose what the start signal does. It is implied that start signal is used to start the operations of the electronic seal but it is not disclosed how the start signal is used, or that it is even used by the device at all.

Claims 10, 11, 12 fail to recite the structural relationships which disclose how the external device of claim 16 is related to the encryption decryption operations or the electronic seal of claim 1. It is unknown how these features are used with the cryptographic operations of claim 1, or if they are used at all by them.

Claim 17 recites that the communication request ID is received from the external device but still does not disclose what the communication request ID is used for, or if it is used in a cryptographic process. Furthermore, the Examiner notes that a communication request ID is not the same as a communication request, or a communication. Unless Applicant's claim makes specific provisions for cryptographically processing using only the communication ID (which it does not), one of ordinary skill in the art would expect the cryptographic methods to employ the processing using the data from the actual communication. This has not been recited in claim 17 or the claims it depends from.

Furthermore, as noted above, the communication request ID is not tied to the functionality of the advance authentication section. It is uncertain whether the communication IDs form the basis for the communications used in the encryption apparatus of claim 14 (in which case this essential subject matter cannot be omitted from the claim) or if the communication ID processing apparatus forms the basis for a completely different apparatus or aspect of the invention (in which case it may be subject to restriction requirement)

Claims 3 fail to recite the structural elements to disclose how the communication request ID is related to the invention. One of ordinary skill in the art would not be able to determine whether the communication request ID is the ID of an internal transaction or memory operation, or whether the communication request ID is the ID of a network transmission. Although the communication ID is used in the production of the start signal, the claims fail to recite how either

of these two bits of information are used within the context of the encryption decryption operations of the electronic seal or if they are even used by the authentication mechanism of claim 14 at all. Furthermore the Examiner notes that all system calls within a computer have a communication ID. "Operating System Concepts" 5th edition pages 64-66.

Claim 6 fails to recite the structural elements interrelating the particular modes to the actual encryption decryption process of claim 1. Furthermore, it is indefinite whether the "determined mode" is a specific mode, or whether or not the "determined" refers to the "considered" mode in light of the fact that there is a "determination key"

Additionally, in light of the disclosure of claim 8, it is uncertain whether the mode exists as an apparatus capable of input/output, or rather it is a mode of execution. As recited above, no disclosure interrelating the different modes of operation is made to the encryption process of claim 1.

Claim 8 recites a registered seal mode section, but fails to disclose how the registered seal mode is related to the authentication and encryption decryption of claim 1. A registered seal mode implies that the section goes through a registration process. No disclosure is made as to how the registered seal mode registers or is registered. It is further indefinite whether the registered seal mode is a physical apparatus such as a memory which outputs a prescribed key, or a mode of operation implied by the recitation of claim 6.

Claim 21 is rejected for the same reasons as claim 8.

Claim 22 is rejected for the same reasons as claim 8.

Claim 23 is rejected for the same reasons as claim 9.

Claim 24 is rejected for the same reasons as claim 10.

Claim 25 is rejected for the same reasons as claim 11.

Claim 26 is rejected for the same reasons as claim 12.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier "Applied Cryptography" pages 41-44, and "How Computers Work", Ron White.

In reference to claim 1:

(Schneier, "Applied Cryptography", pages 41-44) discloses an electronic seal, comprising:

- an input/output section for receiving a random number encrypted based on a prescribed key, where the prescribed key is Bob's public key and the random number is the message. ("Resending the message as a receipt" , p.42, steps 1)

- An advance authentication processing section for decrypting the encrypted and received random number based on a secret key related to the prescribed key and then encrypting the decrypted random number based on the secret key, where the secret key is Bob's private key, and where Bob upon receiving the message decrypts the encrypted message using his private key, and where bob then encrypts the message with the private key by digitally signing it. ("Resending the message as a receipt" , p.42, steps 2 and 3)

- Wherein the input/output section outputs the encrypted random number encrypted based on the secret key, where the step of outputting comprises sending the message back to Alice. ("Resending the message as a receipt" , p.42, steps 3)

Although Schneier does not explicitly recite that the message is a random number, the encryption of a random number, and its subsequent decryption and comparison is well known in the cryptographic arts as a challenge.

For Example US patent, 5481611, Figure 1 discloses the encoding of a random number that is compared. Access is granted if the result of the original challenge and the decrypted returned challenge are the same.

Schneier fails to explicitly disclose any hardware structure to implement the method as described in pages 41-44. The reason no explicit disclosure is made is because those of ordinary skill in the art would understand that the significance of the cryptographic method lies in the software/logical steps it performs rather than any physical realization of that method.

However, the presumption of Schneier as recited in pages 40-44 is that Alice and Bob, are two people communicating through computer clients, wherein each computer client has within it a standard CPU, a RAM, keyboard, etc. Just as the recitation of a car would ordinarily imply that such a car would have an engine, steering wheel, windshield, transmission, etc. so too would the recitation of a computer imply to those of ordinary skill in the art the components of a standard computer system.

For example, step of receiving a random number encrypted would necessitate an input/output section. An output section would be required to send the random number encrypted in the first place, while an input section would be required to receive that random number.

An advance authentication processing section would be required because wherever data must be processed, a processing section must be provided.

The input/output section of outputting the encrypted random number based on the secret key recited by the methods of Schneier must similarly necessitate an input/output processing section.

It would have been obvious to one of ordinary skill in the art to use a standard computer by each of the clients in Schneier pages 40-44 across a network in order to more efficiently implement the cryptographic and algorithmic techniques.

For purposes of clarity, the Examiner has chosen to use the illustrative "How Computers Work" reference by Ron White to disclose the various internal components used by an ordinary computer.

In reference to claim 2:

(Schneier, "Applied Cryptography", pages 41-44) and "How Computers Work" Ron White electronic seal discloses the method according to claim 1, wherein the advance authentication processing section includes:

- A secret key memory section for storing the secret key, where the secret key memory section would be the memory where the data of the encryption process is stored. (pages 42-47) "How RAM works"
- A decryption section for decrypting the encrypted and received random number based on the secret key, where the decryption section is performed in the memory of the clients using the processor to process the cryptographic data. (pages 42-47) "How RAM works & Pages 52-63, and where the cryptographic process that is performed is illustrated in ("Resending the message as a receipt" , p.42)

- An encryption section for encrypting the decrypted random number based on the secret key, where the encryption section is performed in the memory of the clients using the processor to process the cryptographic data. (pages 42-47) "How RAM works & Pages 52-63, and where the cryptographic process that is performed is illustrated in ("Resending the message as a receipt" , p.42)

In reference to claim 4:

(Schneier, "Applied Cryptography", pages 41-44) and "How Computers Work" Ron White electronic seal discloses an electronic seal according to claim 1, wherein:

The random number encrypted based on the prescribed key is output from a memory medium, where the random number would be output from the memory where the data of the encryption process is stored. (pages 42-47) "How RAM works"

The input/output section is a reader/writer section for supplying a power to the memory medium, where the power that is supplied comes in electrical pulses. (pages 42-47) "How RAM works" & (pages 3-5)

In reference to claim 5:

(Schneier, "Applied Cryptography", pages 41-44) discloses an electronic seal according to claim 1, wherein:

- The prescribed key is a public key, where the prescribed key is Bob's public key. ("Resending the message as a receipt" , p.42, steps 1)

- The secret key forms a key pair with the public key based on one of an RSA cryptosystem and an elliptic curve cryptosystem, where the secret key is Bob's private key, and where the cryptosystem involved is an RSA public key cryptosystem. ("Resending the message as a receipt" , p.42, step 2 & p.42 1st paragraph)

In reference to claim 7:

The Examiner takes official notice that rendering an electronic seal where such seal contains an input and output processing section in the shape of one of a card-shape, a cylindrical shape, and a prism shape was known at the time of invention.

In particular, electronic seals with cryptographic processing capabilities are often used as smartcards in the art. The seal is placed on a card, and the card shape provides ease of access in usage and portability by users.

US patent 5544246 discloses an example of a smartcard with cryptographic processing capabilities.

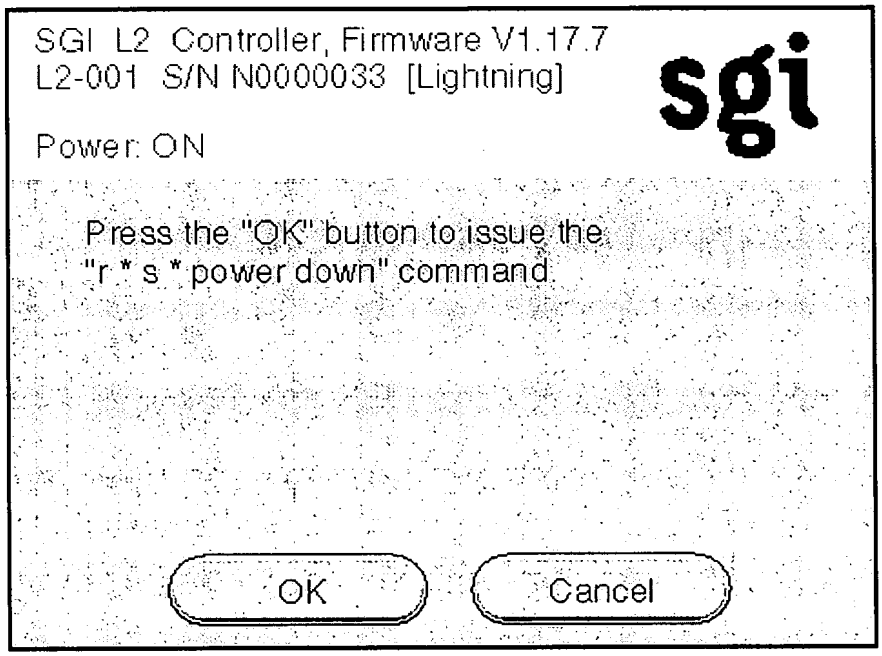
It would have been obvious to one of ordinary skill in the art at time of invention to render the cryptographic processing electronic seal in a card-shape in order to provide ease and portability to users.

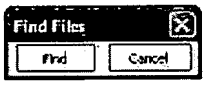
In reference to claim 9:

An electronic seal according to claim 1, further comprising a cancel mode section for canceling a result of advance authentication based on an operation of the advance authentication processing section.

The Examiner takes official notice that the action of canceling a processed result was well known at the time of invention.

For example, when a data process is in execution, users are often given the option to cancel the processing in order to allow for last minutes changes to an operator's desired command of the process.





In telecommunication, the term **cancel character** has the following meanings:

1. A precision control character (In Unicode, the hexadecimal code number is 0x18, abbr is CAN) used to indicate that the data with which it is associated are in error or are to be disregarded.
2. An accuracy control character (In Unicode, the hexadecimal code number is 0x94, abbr is CCH) used to indicate that the data with which it is associated are in error, are to be disregarded, or cannot be represented on a particular device.

It would have been obvious to one of ordinary skill in the art at the time of invention to cancel a result of the advance authentication processing in order to provide greater control of the processing by allowing the operator control of the processing section even after processing has begun.

In reference to claim 13:

An electronic seal according to claim 6, further comprising a clock mode section for displaying the current time on the display section.

The Examiner takes official notice that a clock mode section for displaying the current time on a display screen was well known to those of ordinary skill in the art at the time of invention.

Placing a displaying screen to display the current time on a processing apparatus provides a convenience to the user in letting the user know what time it is. Although the actual processing system may make use of the time in its computations, it need not provide a display to show the current time to use the time information. The display allows convenience to the user even if the user may have other means of ascertaining the time,

Claim 14 is rejected for the same reasons as claim 1.

In reference to claim 15:

(Schneier, "Applied Cryptography", pages 41-44) and "How Computers Work" Ron White electronic seal discloses a memory medium according to claim 14, wherein the advance authentication processing section includes:

- A random number generation section for generating the random number; (page 44 "Random and pseudo random sequence generator")

- A prescribed key memory section for storing the prescribed key, where the prescribed key memory section would be the memory where the data of the encryption process is stored. (pages 42-47) "How RAM works"
- An encryption section for encrypting the generated random number based on the prescribed key, where the encryption section is performed in the memory of the clients using the processor to process the cryptographic data. (pages 42-47) "How RAM works & Pages 52-63, and where the cryptographic process that is performed is illustrated in ("Resending the message as a receipt" , p.42)
- A decryption section for decrypting the random number, encrypted based on the secret key, based on the prescribed key, where the decryption section is performed in the memory of the clients using the processor to process the cryptographic data. (pages 42-47) "How RAM works & Pages 52-63, and where the cryptographic process that is performed is illustrated in ("Resending the message as a receipt" , p.42)
- A comparison result memory section for storing a result of comparison, where the comparison result memory section would be the memory where the data of the encryption process is stored. (pages 42-47) "How RAM works"
- A random number comparison section for comparing the generated random number and the decrypted random number. . (pages 42-47) "How RAM works & Pages 52-63, and where the cryptographic process that is performed is illustrated in ("Resending the message as a receipt Item (4)" , p.42)

Claim 18 is rejected for the same reasons as claim 5.

Claims 19-20 are rejected for the same reasons as claim 15.

Claim 27 is rejected for the same reasons as claims 1 and 2.

Claim 28 is rejected for the same reasons as claim 7.

In reference to claim 30:

A mobile device according to claim 29, wherein the mobile device is a cellular phone detachably accomodating the electronic seal.

The Examiner takes official notice that the use of a mobile device such as a cellular phone detachably accomodating an electronic seal such that the electronic seal is a smartcard with authenticating processing capabilities was well known to those of ordinary skill in the art at the time of invention.

The SIM card is a smartcard placed inside a cellular phone and is typically the piece of memory used to authenticate the user of the phone to the cellular network. The advantage of using this method is so that when a user decides to change phones, he or she can simply remove the SIM card and place it in a newly purchased phone. It is the SIM card which maintains the identity of the user.

For Example:

- US patent 6669487, Figures 1 & 5, et seq.

- US patent 6631840, Figures 3 & 4

It would have been obvious to one of ordinary skill in the art to use a cellular phone to detachably accommodate the electronic seal in order to allow authentication of users on cellular phones, and to allow users to conveniently change phones because the authentication information is confined to the detachable electronic seal.

Conclusion

5. The following art not relied upon is made of record:

- US patent 5802178 discloses a method of regulating computer security in networks using a stand-alone device.
- US patent 5828832 discloses a multilevel network security interface.
- US patent 5469556 discloses a security system for resource access in a stand-alone device.

6. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on **(571)272-3799.**

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 571-273-8300
Customer Service Representative	Telephone: 571-272-2100	Fax: 571-273-8300

TMH

June 13th, 2007